We claim:

1. A method of protecting a network from potentially harmful data traffic traversing a plurality of data ports of the network, the data traffic comprising data packets, the method comprising the steps of:

a. providing a means for monitoring attributes of data traffic traversing a plurality of data ports of a network;

b. providing a means for responding when an attack on said network is determined to occur;

c. defining a set of attack parameters from attributes of one or more data packets traversing a network, such that when said defined set of parameters are met an attack on said network is presumed to occur;

d. specifying a set of responses that may be taken in response to said attack, wherein said responses are defined by a set of response rules, said response rules being designed to select one or more of said responses from said set of specified responses based upon monitored attack parameters;

e. monitoring all the data packets traversing the data ports from a plurality of sources with said monitoring means to determine when said attack parameters have been met;

f. comparing and coordinating said attack parameters and said response rules to select one or more of said set of specified responses based upon said monitored attack parameters; and

g. providing said one or more selected responses through said response providing means to protect said network from said attack.

2. The method of claim 1 wherein said set of responses is selected from the group consisting of a denial of access response, an alert response wherein an alert of said attack is provided, a throttling response wherein data packets are queued and sent along the network at a controlled rate, a redirection response wherein the attack from an attacking source is redirected to another destination, and combinations thereof.

3. The method of claim 1 or 2 wherein said step of comparing and coordinating said attack parameters and said response rules utilizes a Radix tree.

4. The method of claim 1, 2 or 3 wherein said means for monitoring attributes of data traffic traversing a plurality of data ports of a network is through non-promiscuous packet capturing on the firewall device.

5. The method of claim 1, 2 or 3 wherein said means for responding when an attack on said network is determined to occur is through insertion of flow control rules on the firewall device.

6. The method of claim 1 wherein said attributes of said data packets are selected from the group consisting of a data packet's source address, a data packet's destination address, a data packet's source port, a data packet's destination port, the number of data packets from a source address per unit of time; the number of data packets from a source port per unit of time, a data packet's protocol, and combinations thereof.

7. The method of claim 6 where said response is selected based upon said data packet attributes selected from the group

consisting of a data packet's source address, a data packet's destination address, a data packet's source port, a data packet's destination port, the number of data packets from a source address per unit of time; the number of data packets from a source port per unit of time, a data packet's protocol, and combinations thereof.

8. The method according to claim 2 wherein the step of denying access to the source is automatic.

9. The method according to claim 1 further comprising the step of copying each of the data packets for monitoring.

10. The method according to claim 1 wherein the step of monitoring further comprises monitoring both incoming and outgoing data packets traversing the data ports.

11. The method according to claim 1 where the step of monitoring further comprises separately monitoring the data packets traversing each of the data ports.

12. The method according to claim 2 further comprising allowing data packets from sources other than the denied source to traverse the data ports.

13. The method according to claim 2 further comprising allowing packets from protocols other than the denied protocol to traverse the data ports.

14. The method according to claim 1 wherein said response rules are user defined.

15. A system for protecting a network, the system comprising a data monitoring means programmed to sample data packets transmitted to and from the network, a memory for storing the sampled data packets and a processor for comparing and coordinating selected attack parameters based upon attributes

of said data packets and a set of specified responses defined by one or more response rules to select one or more of said set of specified responses based upon said monitored attack parameters and provide said one or more selected responses to protect said network from said attack.

16. The system according to claim 15 wherein said attributes are selected from the group consisting of a data packet's source address, a data packet's destination address, a data packet's source port, a data packet's destination port, the number of data packets from a source address per unit of time; the number of data packets from a source port per unit of time, a data packet's protocol, and combinations thereof.

17. The system according to claims 15 or 16 wherein said response is selected from the group consisting of a denial of access response, an alert response wherein an alert of said attack is provided, a throttling response wherein data packets are queued and sent along the network at a controlled rate, a redirection response wherein the attack from an attacking source is redirected to another destination, and combinations thereof.

18. The system of claim 17 wherein said attack parameters and said response rules are coordinated using a Radix tree.

19. The system of claim 15 wherein said data monitoring means, said memory and said processor are contained within a router.

20. The system of claim 19 wherein said router is one rack unit in height.

21. The system of claim 20 wherein said router is used in combination with a computer firewall.